DOI: 10.31915/NWS.2019.24

A felhasználói viselkedés, mint információbiztonsági kockázat becslése

Leitold Ferenc
Secudit Kft.
fleitold@secudit.com

A felhasználói viselkedés sokkal veszélyesebbé teszi egy szervezet működését, mint bármely technikai sebezhetőség. Számos technikai megoldás létezik a technikai lehetőségeket kihasználó támadásokkal szemben. Az informatikai biztonság technikailag egy jól felkészült védelmet képes biztosítani, ugyanakkor az emberi tényező kezelése még mindig a gyerekcipőben jár. Ez az előadás a felhasználói viselkedés értékelésének lehetséges módszereivel foglalkozik, alapvetően néhány hasznos megfigyelési lehetőség kerül előtérbe, melyek alkalmasak (akár automatikus módon) a felhasználói viselkedés mérésére. A bemeneti források, amiket használhatunk, az adott felhasználó által használt munkaállomásból, a hálózati forgalomból és az alkalmazásnaplókból (különösen a védelmi rendszerek naplóiból) származhatnak. Ezeket a bemeneti forrásokat használva néhány nagyon hasznos metrikát is definiálhatunk a felhasználók viselkedésének megítéléséhez, illetve a felhasználók besorolásához. Miután meg tudtuk mérni a felhasználói magatartás szintjét, használhatjuk azt az adott szervezet informatikai biztonságának javítására is.

A tanulmány a következő részeket tartalmazza:
- Bevezetés a felhasználói viselkedés kezelésébe (mérés és cselekvés),
- Hasznos eszközök a felhasználók viselkedésével kapcsolatos néhány alapvető jel automatikus méréséhez,
- A mért adatok kiszámítása a mért jelekből,
- Mit tehetünk a metrikákkal?

Keywords: vulnerability assessment, user behavior assessment, human factor

Bevezetés

A DVA (Distributed Vulnerability Assessment) technológia a Dunaújvárosi Egyetem és a Secudit közös kutatási munkája alapján jött létre. A DVA részletes leírást ad egy szervezet internetes támadási sebezhetőségeiről. A módszer szerint első lépésként az egyedi felhasználók és az informatikai infrastruktúra elemeinek sebezhetőségét az egyes ismert fenyegetésekre vonatkozóan kell felmérni, majd ezeket az eredményeket kombinálni az adott szervezet számára releváns fenyegetésekre vonatkozóan. A módszer egy adott szervezet integrált kiber-támadási sebezhetőségét a jelenleg ismert fenyegetések elterjedtségét és hatékonyságát; a felhasználók biztonságtudatos viselkedését; és az informatikai infrastruktúra gyengeségeit alapul véve értékeli. Matematikai módszereket alkalmazva az integrált sebezhetőség felbontható arra, hogy az egyes felhasználók, illetve az egyes IT infrastruktúra elemek milyen mértékben járulnak hozzá az integrált sebezhetőséghez, a teljes szervezet fenyegetettségéhez. A DVA-eredményekből a fenyegetettség mennyiségi szempontból hozzárendelhet a

különböző belső hozzájáruló összetevőkhöz (például felhasználói azonosító, portok, protokollok, védelmi rétegek). Ez lehetővé teszi, hogy különböző közreműködő komponenseket összehasonlítható mérőszámokkal értékeljünk (pl. felhasználói biztonságossági tudatosság, az infrastruktúra javításának lehetősége, illetve a rosszindulatú programok elleni védelem hatékonysága alapján). A DVA lehetővé teszi az információbiztonsági menedzserek számára, hogy a "mi lenne, ha" típusú lekérdezések eredményei alapján összehasonlíthassák a különböző rendelkezésre álló lehetőségeket a szervezet fenyegetettségének csökkentése érdekében, amelyek egyébként nem lennének mennyiségi szempontból összehasonlíthatók (pl. további cybersecurity alkalmazások és szolgáltatások.)

A DVA módszer működésének alapfeltétele, hogy a felhasználói biztonságtudatosságot is automatikusan lehessen mérni. Ebben a cikkben a felhasználói biztonságtudatosságra jellemző metrikával foglalkozunk, milyen jellemzők alapján mérhető.

1. Fenyegetettségek modellezése

Ahhoz, hogy egy kártékony támadás sikeres legyen egy védett hálózattal szemben, a kártékony kód sikeres végrehajtása szükséges. A felhasználói oldalon a legegyszerűbb minimális viselkedés nem más, mint a végpont eszköznek az internethez történő csatlakoztatása. Az informatikai biztonsági metrikák manapság a védett IT-re (pl. folyamatos sérülékenység-tesztelés), illetve a kártevők tevékenységére, tulajdonságaira (pl. védelmi rendszerek tesztelése) [6] fókuszálnak. A felhasználói magatartásra vonatkozó informatikai biztonsági metrika kevésbé fejlett [3], habár a hálózati forgalom megfigyelése lehetőséget ad a fejlesztésükre (pl. NetFlow/IPFIX). A passzív figyelés mellett az interaktív metrikát is alkalmazhatjuk [10].

A sikeres kártékony támadásokat a védett környezetben megvalósítható kártékony tevékenység és a megfelelő felhasználói magatartás metszeteként lehet reprezentálni. Ez a koncepcionális keret az NSS Lab által használt működési szabályokra épül [18], ugyanakkor praktikus és kényelmes egyszerűsítése a támadási felületek komplett kezelésének. Az alábbiakban csak a humán-interaktív végpontokra fókuszálunk (IT), a beágyazott rendszerek biztonsági architektúrájával (IoT, OT) jelenleg nem foglalkozunk. Három különálló, de erősen interaktív sérülékenységi forrást veszünk figyelembe:

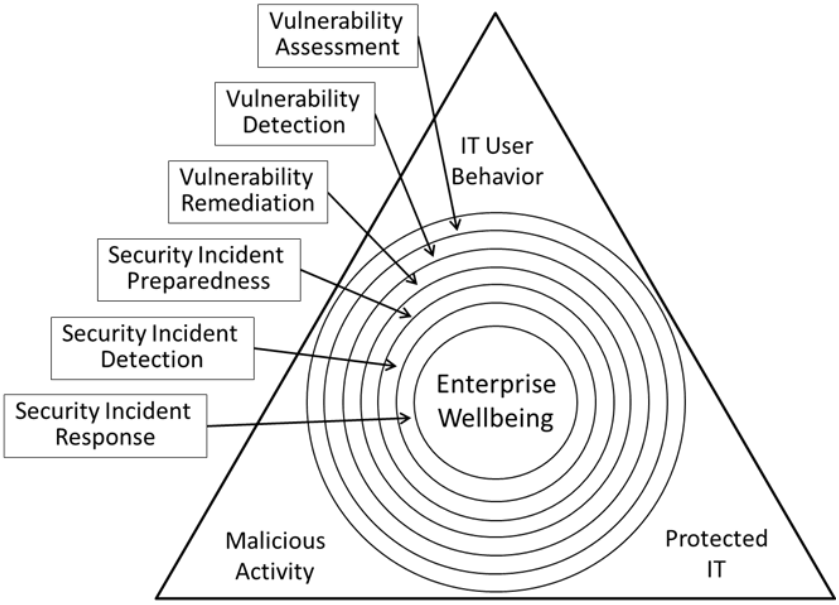
(1) kártékony tevékenység azok által, akik saját céljaikra használják ki a hálózat képességeit, hogy megsértsék a megbízható IT rendszer védelmét;
(2) veszélyes IT felhasználói magatartás (pl. alkalmazottak, vevők, beszállítók); és
(3) védelem nélküli sérülékenység az IT hálózati infrastruktúrában.

A legkritikusabb sérülékenység e három terület közös részében, metszetében található (1. ábra). E sérülékenységek megfelelő láthatóságot, ellenőrzést és megkülönböztetést követelnek a megfigyelésükhöz, megértésükhöz és az ellenük történő hatékony védekezéshez. A meglevő és esetleg felmerülő sérülékenységek láthatóságához éber

1. ábra: Az IT sérülékenység komponenseit és tényezőit három területre lehet osztani, melyek mindegyikének saját módszere és eszközei vannak a láthatóság, ellenőrzés és megkülönböztetés céljára [13]

kockázatelemzés szükséges, ami mindhárom területet figyeli (1. ábra).

Az információs folyamatok sérülékenységeinek láthatósága szükséges, de önmagában elégtelen az informatikai biztonság szempontjából. A sérülékenység értékelése a biztonság biztosításának legkülsőbb rétege. A következő rétegek: sérülékenység érzékelés, sérülékenység javítása, biztonsági incidensre való felkészülés, biztonsági incidens érzékelése, és biztonsági incidensre való reagálás (2. ábra).



2. ábra: Sérülékenység felmérése a teljes biztonság érdekében a szervezet jóléte céljából [13]

A szervezet jólétének biztosításához a sérülékenységek kezelése a sérülékenységek forrásainak gyakorlati és hatékony azonosítását követeli meg. A biztonsági incidensre való reagálás követelményét az esemény információkezelő rendszerek elégítik ki (SIEM). A sérülékenységek hatékony kezeléséhez az informatikai sérülékenység

hármas modellje szükséges. A korábbi szabályokból eredően [11, 12] a hármas modell a sérülékenység mérését 3 forrásra osztja: i) kártékony tevékenység; ii) védelemmel rendelkező IT; és iii) nem megfelelő felhasználói magatartás. Mindegyik forrásban specifikus tényezőket azonosítunk és jellemzünk (pl. vírusküldés és kihasználás a kártékony tevékenységi hármasban). A modell alapot ad a tényezők korrelációjához és kombinálásához a sérülékenységek integrált nézetéhez.

2. A DVA számításának matematikai háttere

Az elosztott fenyegetettség felmérés (DVA) matematikai háttere valószínűségszámításra épül ([19]):
Legyen

$$\mu(t,u) = \frac{number\ of\ attempts\ of\ \mathbf{t}\ are\ enabled\ by\ the\ user\ \mathbf{u}}{number\ of\ attempts\ of\ \mathbf{t}\ are\ enabled\ by\ the\ average\ user}$$

Ekkor

$$p_s(l) = 1 - \prod_{for\ all\ t,u\ and\ i} (1 - p_{user}(t,u) \cdot p_{device}(t,i) \cdot p_{prev}(t,l))^{k(t,u)}$$

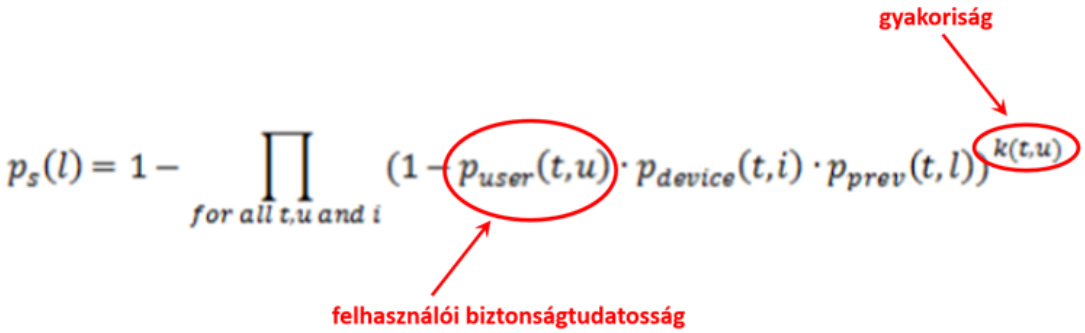
ahol $u \in U,\ i \in I,\ t \in T_l, l \in L$ és

$$k(t,u) = \frac{T}{\Delta T} \cdot \frac{T_u}{T_{average}} \cdot \mu(t,u)$$

ahol

ΔT az elterjedtségekre (prevalence) vonatkozó időintervallum,
T az az időintervallum, amire az általunk számított valószínűségi mérték vonatkozik,
T_u az az időintervallum, amennyi ideig az u felhasználó használja a számítógépet,
$T_{average}$ az az időintervallum, amennyi ideig egy átlagos felhasználó használja a számítógépet, μ (*t,u*) a fentiek alapján számított érték.

A fenti képletben a felhasználói viselkedés az alábbi tényezőkben jelenik meg:



A DVA modell szerint a felhasználói viselkedés két tényező formájában jelenik meg, egy számítógép felhasználónak két lényeges tulajdonsága van, melyek befolyásolják a szervezet veszélyeztetettségi mértékét. Egyrészt a felhasználói biztonságtudatosságra jellemző mérték, mely azt mondja meg, hogy egy adott felhasználó esetén, ha egy bizonyos szituációba kerül milyen valószínűséggel hoz olyan döntést vagy végez olyan tevékenységet, mely aztán a veszély okozta esemény bekövetkezését eredményezi. A másik jellemző tulajdonság arra utal, hogy egy adott felhasználó milyen gyakran kerül olyan szituációba, hogy döntést kelljen hoznia. Ez utóbbi esetben rengeteg olyan eszköz, szolgáltatás áll rendelkezésre, mely képes arra, hogy például a felhasználók be- és kijelentkezési idejét, a szoftverek használatát naplózza. Ebben a cikkben a továbbiakban elsősorban a felhasználói biztonságtudatossággal, annak mérésével, illetve a felhasználói biztonságtudatossági mérték meghatározásával foglalkozunk.

3. Felhasználói biztonságtudatosság mérése

A felhasználói biztonságtudatosság esetén két lényeges kérdés merül fel: egyrészt azt vizsgáljuk meg, hogy melyek azok a mérhető jelek, melyek szoros kapcsolatban vannak a biztonságtudatossággal, illetve a mérési módszer lehetőségeit is megvizsgáljuk.

Mit mérhetünk?

A felhasználói biztonságtudatosság esetén számos olyan mérhető információ áll rendelkezésre, melyek segíthetnek a felhasználói biztonságtudatosságra jellemző mérték meghatározásában. Ilyenek például:

- Eszköz használata
- Alkalmazások használata (főként: kommunikációs alkalmazások)
- Különböző típusú fájlok megnyitása/indítása
- Védelmek befolyásolása (pl.: frissítés, felfüggesztés)
- Böngészés az interneten

Hogyan mérhetünk?

A felhasználói biztonságtudatosság mérésére manuális, kérdőív, tesztjellegű felmérés az általában megszokott módszer. Ennek a legnagyobb hátránya, hogy nem a tényleges viselkedés biztonságosságát méri, hanem azt, hogy a felhasználó

milyen biztonságtudatossági ismeretekkel rendelkezik. Azaz a mérés hibás lesz azokra vonatkozóan, akik pontosan tudják, hogy mi a helyes, biztonságtudatos viselkedés, de nem azt teszik.
A biztonságtudatosság mérése alapvetően két módszerrel képzelhető el:

- A **passzív módszer** révén a felhasználók szokásos viselkedését vizsgáljuk és ebben keresünk olyan jeleket, amelyek olyan magatartásra utalnak, amelyek valamilyen veszély/támadás elhárítását vagy elősegítését jelentik.
- Az **aktív módszer** segítségével szándékosan előidézünk olyan szituációkat, melyekkel valamely veszély/támadás esetén a felhasználói döntést szimuláljuk. Ebben az esetben a felhasználók szokásos viselkedése helyett a felhasználók előidézett szituációkban történő döntését.

Mind a passzív, mind az aktív módszernek megvannak az előnyei és hátrányai. Passzív módszer esetén a felmérés semmilyen módon nem akadályozza a szervezet szokásos működését, míg az aktív módszer esetén ez nem igaz. Az aktív módszer viszont különböző típusú szituációkra vonatkozóan képes a mérést elvégezni, míg a passzív esetben csak olyan szituációk esetén történik ez meg, amelyek ténylegesen előfordulnak.

4. Felhasználói esetek

Amennyiben a felhasználók biztonságtudatos viselkedéséhez valamilyen mérőszámot szeretnénk hozzárendelni, alapvető, hogy ez a mérőszám lehetőséget adjon az összehasonlításra. Az alábbiakban ennek fényében három egyszerű esetet vizsgálunk.

I. eset

Az első esetben a különböző böngészési szokások oldaláról közelítjük meg a felhasználói biztonságtudatosságot. Adott egy felhasználó, aki minden munkanap a böngészőben csak a www.port.hu és a www.idokep.hu oldalakat nyitja meg. Egy másik felhasználó pedig a böngészőjében minden héten legalább 20 olyan weboldalat nyit meg, amit nem látogatott az elmúlt 6 hónapban. Minden egyéb vonatkozásban a két felhasználó viselkedése azonos. Ebben az esetben azt mondhatjuk, hogy a második felhasználó nyilván nagyobb veszélyt jelent, azaz jobban hozzájárul a szervezet veszélyeztetettségi szintjéhez.

II. eset

A második esetben azt mutatjuk meg, hogy akár különböző munkahelyi feladatkörök is befolyásolják a felhasználói biztonságtudatosságot. Adott egy felhasználó, aki a HR osztályon dolgozva, fogadja az álláspályázatokat email-ben és munkaköri feladata, hogy megnyissa a bennük lévő PDF csatolmányokban lévő önéletrajzokat. Egy másik felhasználó pedig soha nem kapott olyan email-t, amiben PDF melléklet lett volna. Minden egyéb vonatkozásban a két felhasználó viselkedése azonos. Ebben az esetben azt mondhatjuk, hogy az első felhasználó nyilván nagyobb veszélyt jelent, azaz jobban, azaz jobban hozzájárul a szervezet veszélyeztetettségi szintjéhez. Ez tehát nem abból adódik, hogy az információbiztonsági tudása alacsonyabb lenne, csupán a munkahelyi feladatköre jelenti a nagyobb kockázatot.

III. eset

A harmadik esetben az első és a második esetet egyesítjük. Adott egy felhasználó, aki a HR osztályon dolgozva, fogadja az álláspályázatokat email-ben és munkaköri feladata, hogy megnyissa a bennük lévő PDF csatolmányokban lévő önéletrajzokat, ugyanakkor a böngészőben csak a www.port.hu és a www.idokep.hu oldalakat nyitja meg. Egy másik felhasználó pedig soha nem kapott olyan email-t, amiben PDF melléklet lett volna, ugyanakkor a böngészőjében minden héten legalább 20 olyan weboldalat nyit meg, amit nem látogatott az elmúlt 6 hónapban. Minden egyéb vonatkozásban a két felhasználó viselkedése azonos. Ebben az esetben nem tudjuk egyértelműen megállapítani, hogy melyik felhasználó jelent nagyobb veszélyt a szervezet számára. Ezt akkor tudnánk megtenni, ha ismerjük azokat a veszélyforrásokat, amelyek emailben, PDF csatolmányokban terjednek, illetve azokat a veszélyforrásokat, amelyek a böngészési szokásokra építenek.

5. Összegzés

A fentiekben módszert mutattunk be a sérülékenység mérésére. Három információforrást használunk: külső informatikai fenyegetés intelligencia („biztonsági intelligencia"), szervezeti IT infrastruktúra gyengeség („behatolás tesztelés"), és a felhasználók fogékonysága, naivsága a támadásokra („felhasználói magatartás"). A módszer lehetővé teszi a mért források kombinálását egy metrikába, amit összevethető sérülékenységekre bonthatunk. A módszer számszerűsíti a relatív sérülékenység evolúcióját időben, külön mérheti az egyedi osztályok (LAN) sérülékenységét és a specifikus fenyegetéseket (pl. zsaroló vírusok, adathalászat). A módszer előrejelzi a potenciális javítási tevékenység következményeit („Mi lesz, ha?"), ezáltal segíti a biztonsággal kapcsolatos döntéshozatalt az adott helyzetben.

A programozott fenyegetések száma manapság 7-800 millió körüli, az aktív támadások köre folyamatosan változik, ráadásul a támadások kb. 90%-át egyedi fertőzések okozzák. Ilyen körülmények között az egy szervezetre vonatkozó veszélyeztetettség mérése sokkal inkább becslés, mint pontos számítás. A bemeneti adatok minél pontosabb meghatározásával, a figyelembe vett kártevők körének kiválasztásával pontosabbá tehető az analízis.

A módszer egyik legfontosabb összetevője a felhasználói viselkedés mérése. A 4. fejezetben leírtak szerint azonban a felhasználói biztonságtudatosság nem csupán egy felhasználóra jellemző metrika, hanem ezt veszélyforrásonként kell meghatározni az egyes felhasználók vonatkozásában. Ennek érdekében a viselkedésre vonatkozó jeleket, jelzéseket kell mérni, majd ezek segítségével határozhatjuk meg a különböző támadási vektorok vonatkozásában a felhasználókra jellemző metrikákat. Minden, a felhasználók viselkedésére vonatkozó mérés természetszerűleg felveti a GDPR vonatkozását is. A GDPR szempontjából a felhasználói viselkedésre vonatkozó mérések, egy szervezet veszélyeztetettségi előrejelzése az információbiztonság javításának az irányába tett lépésnek tekinthető és így a GDPR céljait szolgálja. Természetesen a GDPR-nak megfelelően a módszer csakis az arányosság elvét szem előtt tartva és a felhasználók megfelelő tájékoztatásával alkalmazható.

Irodalom

[1] ARROTT, A., F. Lalonde Levesque, D. Batchelder, and J.M. Fernandez. "Citizen cyber-security health metrics for Windows computers". Proceedings of Eastern European eGov Days Conference, EEGOV, Budapest, Hungary. 2016.

[2] BATCHELDER, D., et al. "Microsoft Security Intelligence Report." Volume 18: July-December 2014, Microsoft, 2015.

[3] CHAPMAN, M.T., "Establishing metrics to manage the human layer." ISSA Security Education Awareness Special Interest Group, 2013.

[4] CLEMENTI, Andreas, Peter Stelzhammer, and Fernando C. Colon Osorio. "Global and local prevalence weighting of missed attack sample impacts for endpoint security product comparative detection testing." Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on. IEEE, 2014.

[5] COLON OSORIO, F.C., and A. Arrott. "Fabric of security - changing our theory and expectations of modern security". Proceedings of Eastern European eGov Days Conference, EEGOV, Budapest, Hungary. 2016.

[6] EDWARDS, S.E., R. Ford, and G. Szappanos., "Effectively testing APT defenses". Virus Bulletin Conference, Prague, Czech Republic, 2015.

[7] KLEINER, A., P. Nicholas, K. Sullivan, "Linking Cybersecurity Policy and Performance, Microsoft Trustworthy Computing", 2013,

[8] KSHETRI, Nir. "Cybercrime and Cybersecurity in the Middle East and North African Economies." Cybercrime and Cybersecurity in the Global South. Palgrave Macmillan UK, 2013.

[9] LALONDE LEVESQUE, F., A. Somayaji, D. Batchelder, and J.M. Fernandez. "Measuring the health of antivirus ecosystems." Malicious and Unwanted Software (MALWARE), 2015 10th International Conference on. IEEE, 2015.

[10] LALONDE LEVESQUE, F., J. M. Fernandez, and A. Somayaji. "Risk prediction of malware victimization based on user behavior." Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on. IEEE, 2014.

[11] LEITOLD, F and K. Hadarics. "Measuring security risk in the cloud-enabled enterprise." Malicious and Unwanted Software (MALWARE), 7th International Conference on Malicious and Unwanted Software, pp: 62-66, ISBN: 978-1-4673-4880-5. 2012.

[12] LEITOLD, F. "Security Risk analysis using Markov Chain Model." 19th Annual EICAR Conference, Paris, France. 2010.

[13] LEITOLD, F., A. ARROTT and K. HADARICS, "Quantifying cyber-threat vulnerability by combining threat intelligence, IT infrastructure weakness, and user susceptibility" 24th Annual EICAR Conference, Nuremberg, Germany, 2016

[14] LEITOLD, F., A. ARROTT and K. HADARICS, "Automating visibility into user behavior vulnerabilities to malware attack" Proceedings of the 26th Virus Bulletin International Conference (VB2016), pp. 16-24, Denver, USA, 2016.

[15] MICROSOFT. "Evolution of malware and the threat landscape - a 10-year review". 2012.

[16] MICROSOFT. "Malicious Software Removal Tool (MSRT)". Microsoft Knowledge Base, article KB890830 revision 161.2, https://support.microsoft.com/en-us/kb/890830

[17] RUBENKING N., "Why Microsoft Doesn't Need Independent Antivirus Lab Tests". PC Magazine, 28 October 2013.

[18] SHAH P, Phatak V, Scipioni R, inventors. "Adaptive intrusion detection system." United States patent application US 10/443,568. 2003 May 22.

[19] LEITOLD, F and K. Hadarics. "Elosztott fenyegetettség felmérés" Networkshop Konferencia, Eger, 2018.